UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,218	11/26/2001	Pasi Into Loukas		8034

7590   04/04/2006

Pasi Loukas
Kemintie 969
Rovaniemi,   96700
FINLAND

EXAMINER
CHEN, SHIN HON

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>17 February 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>28,29,31 and 33-54</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>28,29,31 and 33-54</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>26 November 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 28, 29, 31, and 33-54 have been examined.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.   Claim 46 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention.

4.   Claim 46 recites the limitation "the pertinent client" in line 2. There is insufficient

antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5.   Claims 45 and 46 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by

Bates et al. U.S. Pat. No. 6785732 (hereinafter Bates2).

6.   As per claim 45, Bates2 discloses network based download information system especially

for wide area networks, like the Internet, comprising: client computer(s) (Bates2: summary of

invention); a register host computer which keeps for each client a client-specific download

details register about the web content which the client has acquired from the network (Bates2: column 12 lines 37-58: logging virus information); on the basis of a reiterated updated security check on a same web content which download details has been stored earlier in said register, the register host revising the security risk status for said web content (Bates2: column 12 lines 37-58); wherein the web content comprises files or any data which a client can acquire from the network (Bates2: column 12 lines 37-58).

7.   As per claim 46, Bates2 discloses the system of claim 45. Bates2 further discloses wherein the pertinent client is informed about said revised security risk status (Bates2: column 12 lines 50-58); wherein the client destroys the host appointed web content and/or performs a virus scan (Bates2: figure 9).

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9.   Claims 28, 29, 31, 33-34, 36-44, and 48-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen et al. U.S. Pub. No. 20030191957 (hereinafter Hypponen) in view of Bates et al. U.S. Pat. No. 6785732 (hereinafter Bates2).

10.   As per claim 28, Hypponen discloses network based web content identification and

control system for wide area networks, like the Internet, comprising: : client computer(s), which

are any computers in the network (Hypponen: [0006]-[0010]); examiner host computer(s), which

are remote third-party computers in the network (Hypponen: [0036]: virus scanning server);

performing an remote identity check on web content (Hypponen: [0036]: check if the content

contains virus); wherein the identity check is performed by an examiner host in response to a

remote service request (Hypponen: [0009]-[0010]: virus scanning server receives data to be

scanned from intermediate servers); wherein the examiner host returns the results of said identity

check as a feedback, and on the basis of said results: (a) it is performed safety measures, (b)

and/or, said client computer and/or the user of said client computer is informed about the results

of said comparison, (c) or, no specific actions are performed (Hypponen: [0006]-[0010] and

[0035] and [0038]: intercept the data and identify if the data is of a type capable of containing a

virus); wherein said web content comprises files, web pages, e-mail messages, e-mail message

attachments or any data which a client computer can acquire from the network (Hypponen:

[0032]). Hypponen does not explicitly disclose performing an on-demand remote identity check

on a specially established tiny-sized independent identification of the web content, what is used

as a preferred method of processing rather than processing said web content as such; wherein

said identification is a data object which is based on certain property(ies) of said web content so

that a unique representation of the identity of said web content is established; wherein said

identification is delivered without said web content for said identity check, in response to a client

direct request to receive said web content from the network. However, Bates2 discloses a web

server includes virus control mechanism that is able to examine whether files are virus-infected

upon user preferences "on-demand" (Bates2: column 5 line 65 – column 6 line 20 and column 8

lines 35-36: the user can decide whether to check the files automatically by the web server or

upon specific user request) and the virus control mechanisms comprises virus information

database that include a specification of known viruses, along with statistics of which ones have

been encountered and a list of web sites (URLs) that are known to contain viruses (Bates2:

column 6 lines 10-20: URLs are tiny-sized identification of data). It would have been obvious to

incorporate the functionality of the virus scanning mechanism of the Bates2 within the virus

server of Hypponen and users to specify virus checking preference on web server to determine

whether the file should be virus checked during transport or upon specific request by the user

because virus mechanism can be individually operated or incorporated within a server module as

well known in the art. Therefore, it would have been obvious to one having ordinary skill in the

art to combine the teachings of Bates2 within the system of Hypponen because it provides user

flexibility in determining virus checking preference and support different types of virus checking

methods.

11.   As per claim 29, Hypponen as modified discloses a network based anti-virus system

according to claim 28. Hypponen as modified further discloses wherein said identity check

comprises the examiner host comparing the delivered identification to store identifications of

web content (Bates2: column 6 lines 10-20: compare the URLs).

12.   As per claim 31, Hypponen as modified discloses a network based anti-virus system

according to claim 28. Hypponen further discloses the system comprising: wherein said

delivered identification consists of file identification information and/or, data identification

information (Bates2: column 6 lines 10-20; column 8 lines 23-44); wherein a said stored

identification consists of file identification information and/or, data identification information

(Bates2: column 6 lines 10-20); wherein said file identification information comprises one or

more of the following properties of the file or other web content to which said file identification

belongs: (a) source URL-address or other type of address, (b) source computer URL-address or

other type of address, (c) name, (d) type, (e) content type, (f) size, (g) creation date, (h) version

number, (i) publisher, (j) authentication certificate, (k) or, other properties (Bates2: column 6

lines 10-20); wherein said data identification information of the file or other web content to

which said data identification belongs, comprises: (a) a check-sum or any identification value

based upon the data of said file or other web content. (b) and / or, data sample picked according

to a certain pattern, algorithm or other rule from said file or other web content, (c) or, all data of

said file or other web content (Hypponen: [0035]; Bates2: column 6 lines 10-20); wherein said

file identification information and said data identification information is delivered to said

anti-virus host computer either: (a) solely from said client computer, (b) solely from the

respective source host computer(s) of said file(s) or other web content which file identification

information anal data identification information it is question of, (c) or, partly from said client

computer and partly from said respective source host computer(s) (Hypponen: [0006]-[0010]).

13.   As per claim 33, Hypponen as modified discloses a system according to claim 29.

Hypponen as modified further discloses wherein said stored identification belong to known virus

infected web content (Bates2: column 6 lines 10-20).

14.   As per claim 34, Hypponen discloses a system according to claim 33. Hypponen further discloses the system comprising: wherein said safety measures including one or more of the following: (a) preventing the download of the examined web content to the client computer, (b) performing a virus scan on the examined web content in the client computer or in the examiner host computer, (c) destroying the examined web content (Bates2: column 6 lines 39-49).

15.   As per claim 36, Hypponen discloses a system according to claim 33. Hypponen further discloses the system comprising: intermediate computer(s), which are any computers in the network capable to intercept data which client computers receiver from the network (Hypponen: [0035]); wherein said delivered identification(s) is delivered to the examiner host computer by a said intermediate computer (Hypponen: [0035]-[0038]).

16.   As per claim 37, Hypponen discloses a system according to claim 36. Hypponen further discloses the system comprising: wherein said safety measures include one or more of the following: (a) the intermediate computer preventing the download of the examined web content to the client computer, (b) the intermediate computer performing a virus scan on the examined web content, (c) the intermediate computer destroying the examined web content (Hypponen: [0035]-[0038]).

17.   As per claim 38, Hypponen discloses a system according to claim 36. Hypponen further discloses the system comprising: wherein said intermediate computer is (a) a server of the local

area network, (b) a server of the internet service provider, (c) or a network node computer

(Hypponen: [0013]).

18.   As per claim 39, Hypponen as modified discloses a system according to claim 29.

Hypponen as modified further discloses wherein said stored identifications belong to known non-

wanted web content (Bates2: column 6 lines 10-20).

19.   As per claim 40, Hypponen as modified discloses a system according to claim 39.

Hypponen as modified further discloses wherein said preventive measures include preventing the

download of the examined web content to the client computer, and/or destroying the examined

web content (Hypponen: [0035]-[0038]; Bates2: column 6 lines 39-49).

20.   As per claim 41, Hypponen as modified discloses a system according to claim 39.

Hypponen as modified further discloses the system comprising: intermediate computer(s) , which

are any computers in the network capable to intercept data which client computers receive from

the network (Hypponen: [0035]); wherein said delivered identification(s) is delivered to the

examiner host computer by a said intermediate computer (Hypponen: [0035]-[0038]).

21.   As per claim 42, Hypponen as modified discloses a system according to claim 41.

Hypponen as modified further discloses the system comprising: wherein said preventive

measures include the intermediate computer preventing the download of the examined web

content to the client computer, and/or the intermediate computer destroying the examined web

content (Hypponen: [0035]-[0038]; Bates2: column 6 lines 39-49).

22.   As per claim 43, Hypponen as modified discloses a system according to claim 41.

Hypponen as modified further discloses wherein a said intermediate computer is: (a) a server of

the local area network, (b) a server of the Internet service provider, (c) or, a network node

computer (Hypponen: [0013]).

23.   As per claim 44, Hypponen as modified discloses a system according to claim 28.

Hypponen as modified further discloses wherein said client computers are host computers into

which data is uploaded (Hypponen: [0031]).

24.   As per claim 47, Hypponen as modified discloses the system of claim 29. Hypponen as

modified further discloses wherein said safety or preventive measures are performed when said

comparison yields a confirmed match (Bates2: column 6 lines 39-49).

25.   As per claim 48, Hypponen as modified discloses a system of claim 47. Hypponen as

modified further discloses wherein if said comparison does not yield a definite match, then a

close enough resemblance of the delivered identification to any of the stored identification(s) is

deemed to be a confirmed match (Bates2: column 12 lines 59-65).

26.   As per claim 49-54, claims 49-54 encompass the same scope as claims 28-44. Therefore,

claims 49-54 are rejected based on the same reasons set forth above in rejecting claims 28-44.

27.   Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen in

view of Bates2 and further in view of Bates et al. U.S. Pat. No. 6721721 (hereinafter Bates).

28.   As per claim 35, Hypponen as modified discloses a system of claim 34. Hypponen does

not explicitly disclose the system comprising: wherein the examiner host computer calculates an

estimate for the security threat level of the examined web content and informs it to the client

computer or the user of the client computer. However, Bates discloses determine trustworthiness

of a file (Bates: column 10 lines 9-39). It would have been obvious to one having ordinary skill

in the art to allow the examiner host computer to determine whether a file poses threat or not

before being transmitting the file to the client. Therefore, it would have been obvious to one

having ordinary skill in the art at the time of applicant's invention to combine the teachings of

Bates within the combination of Hypponen-Bates2 because it allows files to be analyzed prior to

being forwarded to client.

Response to Arguments

29.   Applicant's arguments with respect to claims 28, 29, 31, 33-54 have been considered but

are moot in view of the new ground(s) of rejection.

Conclusion

30.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

Waldin et al U.S. Pat. No. 6094731 discloses comparing hash values of files for virus

detection.

Le Pennec et al. U.S. Pat. No. 6976271 discloses virus-free certificate used to detect

whether a file is infected with virus by examining the certificate associated with the file. One

with ordinary skill in the art would use the virus-free certificate in the Hypponen-Bates2

combination to enable additional virus detecting protocol.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The

examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen

CHRISTOPHER REVAK
PRIMARY EXAMINER

Cll 4/2/06

Examiner
Art Unit 2131

SC